Zeitschrift für Datenrecht und Informationssicherheit

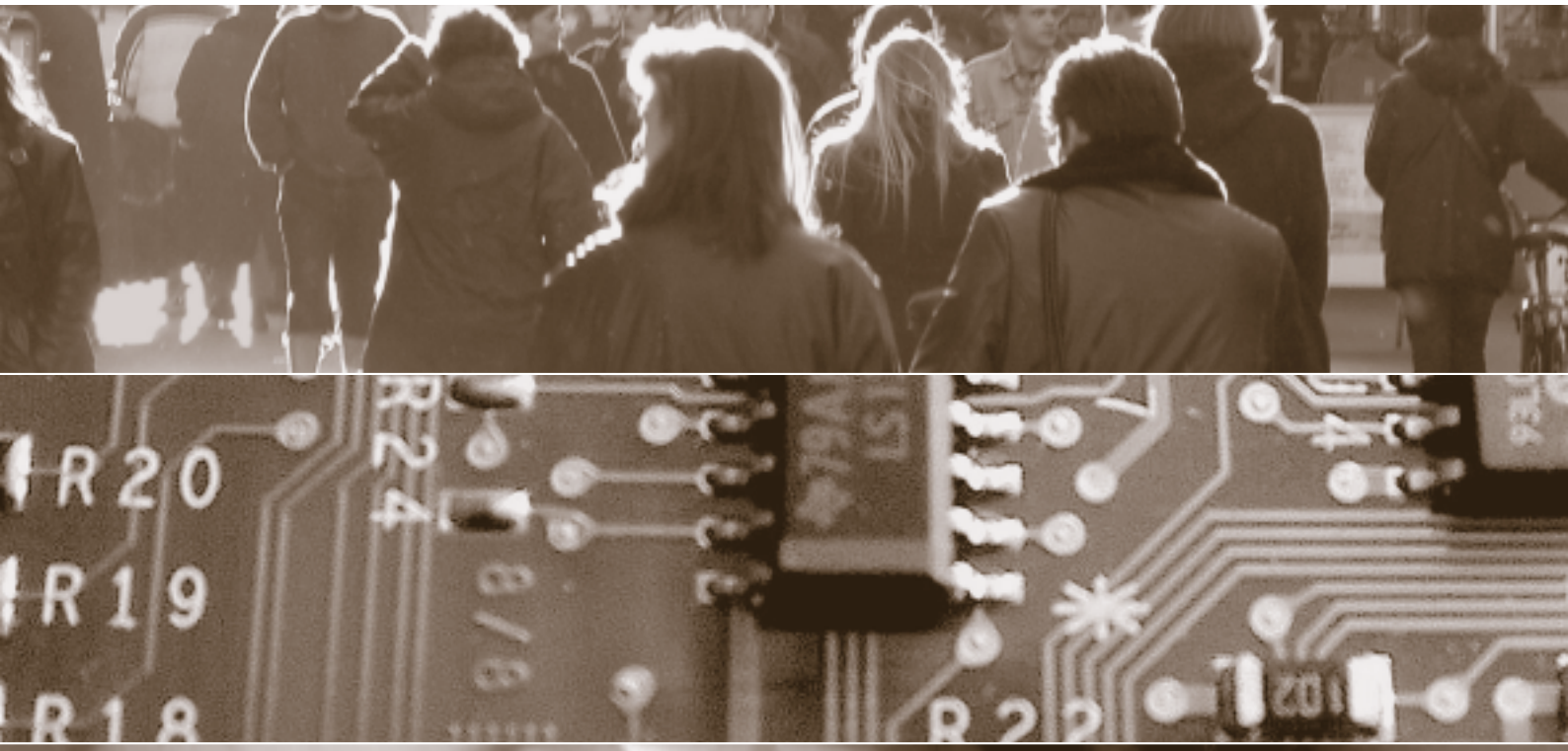
digma

www.digma.info 8. Jahrgang, Heft 1, März 2008

Schwerpunkt:

Anonymisierung

fokus: Das Recht auf Anonymität
fokus: Sind anonymisierte Daten anonym genug?
report: Drahtlose Sensornetze – eine Herausforderung



Herausgegeben von
Bruno Baeriswyl
Beat Rudin
Bernhard M. Hämmerli
Rainer J. Schweizer
Günter Karjoth

Schulthess §

inhalt

fokus

Schwerpunkt:
Anonymisierung

Das Recht auf Anonymität

Das Recht auf Anonymität ist ein Teil des Grundrechts auf informationelle Selbstbestimmung. In der Gesetzgebung finden wir etliche Gewährleistungen. Doch auch ausserhalb dieser Bereiche könnten mit Anonymisierungs- oder Pseudonymisierungslösungen in vielen Fällen die verfolgten Zwecke erreicht werden.

Anonymisierung von genetischen Daten?

Anonymisierung verhindert die Verletzung von Persönlichkeitsrechten. Ist das eine Lösung im Zusammenhang mit Biobanken? Jegliche Verwendung von Daten in einer Biobank setzt eine angemessene Aufklärung voraus.

Sind anonymisierte Daten anonym genug?

Wann reicht eine Anonymisierung aus, damit aus den anonymisierten Daten nicht doch wieder auf die betroffenen Personen zurückgeschlossen werden kann – und die Daten für den Forschungszweck trotzdem noch aussagekräftig genug sind?

Anonymes E-Voting – eine Illusion?

In der Theorie kann anonymes E-Voting mit Hilfe von blinden Signaturen relativ einfach realisiert werden. In der Praxis muss bei einer konkreten Realisierung eines E-Voting-Systems insbesondere darauf geachtet werden, dass nicht über verdeckte Kanäle Informationen über stimmberechtigte Personen z. B. in Tokens hineincodiert werden können.

impressum

digma: Zeitschrift für Datenrecht und Informationssicherheit, ISSN: 1424-9944, Website: www.digma.info

Herausgeber: Dr. iur. Bruno Baeriswyl, Dr. iur. Beat Rudin, Prof. Dr. Bernhard M. Hämmerli, Prof. Dr. iur. Rainer, J. Schweizer, Dr. Günter Karjoth

Redaktion: Dr. iur. Bruno Baeriswyl und Dr. iur. Beat Rudin

Rubrikenredaktor: Dr. iur. Amédéo Wermelinger

Zustelladresse: Redaktion digma, c/o Stiftung für Datenschutz und Informationssicherheit, Kirschgartenstrasse 7, CH-4010 Basel
Tel. +41 (0)61 270 17 70, redaktion@digma.info

Erscheinungsplan: jeweils im März, Juni, September und Dezember

Abonnementspreise: Jahresabo Schweiz: CHF 158.00, Jahresabo Ausland: Euro 112.00 (inkl. Versandspesen), Einzelheft: CHF 42.00

Anzeigenmarketing: Publimag AG, Europastrasse 30, Postfach, CH-8152 Glattbrugg
Tel. +41 (0)44 809 31 11, Fax +41 (0)44 809 32 22, www.publimag.ch, info@publimag.ch

Herstellung: Schulthess Druck AG, Arbenzstrasse 20, Postfach, CH-8034 Zürich

Verlag und Abonnementsverwaltung: Schulthess Juristische Medien AG, Zwingliplatz 2, Postfach, CH-8022 Zürich
Tel. +41 (0)44 200 29 99, Fax +41 (0)44 200 29 98, www.schulthess.com, zs.verlag@schulthess.com

Die Crux der Auskunft über Verstorbene

Die Verordnungsregelung zur Herausgabe von Daten an die Angehörigen von Verstorbenen ist anspruchsvoll, weil sie eine Interessenabwägung voraussetzt. Unter welchen Voraussetzungen ist ein Privatversicherer zur Auskunft an die Angehörigen berechtigt? Wann besteht eine Pflicht dazu?

Datenschutz und wirtschaftliche Realität

Unter welchen Voraussetzungen kann die Wirtschaft Datenschutz realistischerweise umsetzen? Der Diskussionsbeitrag aus dem Kreis des Vereins Unternehmens-Datenschutz fordert mehr Anreize (z. B. Steuererleichterungen) für erwiesenermassen datenschutzkonform handelnde Unternehmen. Steuererleichterung für die Einhaltung von Gesetzen – eine aus Sicht der Redaktion etwas realitätsfremde Forderung.

Drahtlose Sensornetze – eine Herausforderung

Drahtlose Sensornetze werden als die nächste Technologiewelle nach RFID gehandelt. Dabei offenbaren die im Beitrag erörterten Anwendungsfelder, dass es ratsam ist, datenschutzrechtliche, aber auch ethische Fragestellungen frühzeitig zu erörtern.

Europarechtliche Herausforderungen

Bund und Kantone stehen zurzeit im Evaluationsverfahren der EU im Hinblick auf die Assoziation der Schweiz an Schengen/Dublin. Passend dazu ist ein Buch erschienen, das umfassend die europarechtlichen Vorgaben darstellt, nach denen sich das schweizerische Datenschutzrecht künftig zu richten hat.

report

forum

Transfer

Wie ist die Lage in der Informationssicherheit?

Roland Portmann, Leiter Kompetenzzentrum Informations- und Softwaresicherheit, Hochschule Luzern – Technik & Architektur roland.portmann@hslu.ch

Ein Ausschnitt aus den Heise Security News vom 14. Dezember 2007:

- XSS Schwachstelle auf Bundesregierung.de
- F-Secure-Forum gehackt
- Sicherheitsupdate für kritische Lücke in HP-Notebooks
- Manipulation an Squirrel-Mail-Paketen entdeckt
- Mehrere kritische Sicherheitslücken in Apples QuickTime …

Jeden Tag erscheinen solche und ähnliche Meldungen in den entsprechenden Foren. Sie müssen zum Schlusse führen, dass mit aktuellen Patches aller Betriebssysteme und Applikationen, guten Virenscannern und restriktiv konfigurierten Firewalls die wesentlichen Probleme der IT-Sicherheit gelöst werden können. So ist auch die Aussage eines IT-Verantwortlichen nachvollziehbar, der auf ein Schema einer äusserst komplexen Firewall-Infrastruktur zeigt und behauptet: «Wir haben unsere IT-Security im Griff».

Diese Meinung spiegelt sich auch in Ausbildungen im Umfeld von IT-Security wider. Die meisten IT-Security-Ausbildungen, sei es von Fachhochschulen, Universitäten oder anderen Organisationen beschränken sich auf technische Aspekte der IT-Sicherheit. Man lehrt, wie man sich von Hackern und Viren schützt.

Eine gute abgestützte Beurteilung der Bedrohungen beim Betrieb von IT-Anlagen wird regelmässig in Lageberichten der Zeitschrift «kes» veröffentlicht (siehe unter Links). Dieser Lagebericht wird mit Unterstützung von Microsoft erstellt. Er basiert auf Umfragen in mittleren und grösseren Firmen. Gefragt wird nach den tatsächlichen Ereignissen und Schäden im letzten Jahr. Die grösste Bedrohung in den letzten Umfragen war immer: «Irrtum und Nachlässigkeit eigener Mitarbeiter». Interessant waren auch jeweils die Antworten auf die Frage, wie sich die Bedrohungen in Zukunft entwickeln werden. Man war in den letzten Umfragen immer sicher, dass man die Probleme mit den Mitarbeitern in den Griff bekommt, dass aber die Bedrohungen durch Malware stark ansteigen werden. Diese Erwartungen wurden nicht erfüllt – im Gegenteil: In der letzten Umfrage wurde sogar von einer Entspannung an der Malware-Front gesprochen. Damit ist und bleibt der Mitarbeiter die grösste Bedrohung.

Wie schützt man sich vor den Mitarbeitern?

Bei dieser Bedrohungskategorie geht es um Schäden durch Irrtum und Nachlässigkeit. Schäden durch mutwillige Manipulationen (z. B. Weiterleiten von vertraulichen Informationen an die Konkurrenz, Vandalismus) werden in anderen Schadenkategorien subsumiert. Die meisten Schäden dürften von den eigenen Administratoren verursacht werden. Die stark zunehmende Komplexität der IT-Infrastrukturen überfordern zunehmend auch gut ausgebildete IT-Spezialisten. Die in grossen IT-Infrastrukturen anfallenden Fehlermeldungen haben ein Ausmass angenommen, das es zunehmend verunmöglicht, die relevanten Informationen zu identifizieren und zu korrekt zu interpretieren. Der Betrieb von komplexen IT-Infrastrukturen wird zur Glücksache. Die Erfahrung in vielen Firmen zeigt, dass mit einem gut funktionierenden Information Security Management System (ISMS) die Schadenshäufigkeit massiv gesenkt werden kann. Klare Prozesse und Konzepte für den Betrieb der IT-Infrastrukturen helfen diese Bedrohung in den Griff zu bekommen.

Eine weitere Gefahrenquelle sind auch die normalen IT-Anwender, sei es im sorglosen Umgang mit Informationen und mit mobilen Devices, sei es durch falsche Bedienung von Applikationen oder im leichtsinnigen Umgang mit ihren Passwörtern. Viele dieser Bedrohungen lassen sich mit Awareness-Kampagnen senken. Auch mit den häufig sehr kreativen Awareness-Kampagnen lassen sich die Probleme aber nur teilweise lösen. Daher müssen in allen Organisationen die Awareness-Kampagnen mit technischen Massnahmen ergänzt werden. Dazu müssen sehr häufig unpopuläre Einschränkungen für die Mitarbeiter implementiert werden (z. B. keine administrative Berechtigungen auf den Arbeitsplätzen, eingeschränkter Zugang zum Internet). Auch andere Sicherheitsmassnahmen, wie beispielsweise Authentisierung mit Smartcards werden nur widerwillig akzeptiert.

Das Ausbildungsproblem

In vielen Firmen wird die Lösung der Informationssicherheitsprobleme auf die IT-Spezialisten abgeschoben. Diese Fachleute haben in der Regel ein grosses Know-how in allen technischen Aspekten der IT-Sicherheit, jedoch nicht in den Management-Aspekten der IT-Sicherheit. Diese Thematik wird in den meisten Ausbildungen nie thematisiert. Dies führt dazu, dass in vielen Organisationen die IT-Sicherheit als eine rein technische Disziplin betrachtet wird. Da die Umsetzung eines ISMS die Arbeitsweise der IT-Spezialisten stark reglementieren kann, kann die Motivation zur Etablierung eines solchen Systems zudem nicht sehr gross sein.

Das Management-Problem

In vielen Organisationen betrachtet das Management die IT-Sicherheit als eine ausschliesslich technische Disziplin und verlangt von den Fachabteilungen, dass sie mit minimalen Kosten alle Sicherheitsprobleme lösen. Der Betrieb von IT-Infrastrukturen ist immer mit Risiken verbunden und das Management müsste daher bestrebt sein, selbst zu entscheiden, wie mit den Risiken umgegangen wird. Das Management ist in vielen Fällen aber nicht in der Lage, die IT-Risiken zu verstehen und korrekt zu interpretieren.

Das Malware-Problem

Nach den eigenen Mitarbeitern ist gemäss der «kes»-Studie die Malware die zweitgrösste Bedrohung. In der Studie wird ausgeführt, dass die Schadenshäufigkeit im letzten Jahr signifikant zurückgegangen ist. Das ist erstaunlich, da die technische Raffinesse der Malware im gleichen Zeitraum stark gestiegen ist. Der Rückgang dürfte auf sicherere Betriebssysteme und stark verbesserte Schutzmechanismen (Anti-Malware-Produkte) und grosse Fortschritte im Betrieb von IT-Anlagen zurückzuführen sein, wie schnelles Patchen von Servern, sehr häufiges Aktualisieren der Virensignaturen, gute konfigurierte Firewalls.

Die «kes»-Studie beruht im Wesentlichen auf einer Umfrage. Die gemäss dem Lagebericht von Melani stark zunehmenden gezielten Industriespionageangriffe, bei denen nach dem Angriff alle Spuren verwischt werden, dürften nicht in diese Studie einfliessen, da diese Angriffe in der Regel nicht entdeckt werden. Sehr häufig basieren solche professionelle Angriffe auf den Herstellern noch nicht bekannten Schwachstellen von verbreiteten Applikationen wie beispielsweise Office-Produkten von Microsoft. Dies wird erleichtert, da in vielen Firmen regelmässig Sicherheitspatches für die Betriebssysteme, nicht aber für die Applikationen eingespielt werden.

Heute sind zunehmend gezielte Angriffe auf einzelne Personen festzustellen. Gemäss dem (unter Links erwähnten) Report von Messagelabs gelten fast 30% der Angriffe dem Chief Investment Officer und 10% dem CEO.

Lucerne University of
Applied Sciences and Arts

HOCHSCHULE
LUZERN

Technik & Architektur
CC Informations- & Softwaresicherheit

Zusammenfassung

Es kann zusammenfassend gefolgert werden, dass die Schäden von eigenen Mitarbeitern nach wie vor stark unterschätzt werden. Diese Schäden können nur mit einem gut funktionierenden Information Security Management System in den Griff bekommen werden. Die am meisten gefürchteten Schäden durch klassische Malware sind kleiner als erwartet. Über die neue Bedrohung der gezielten Angriffe, die von den Firmen in der Regel nicht entdeckt werden, gibt es keine gesicherten Statistiken. Die Meldestelle Melani des Bundes sieht in der Industriespionage eine grosse Bedrohung der schweizerischen Industrie. ■

Weiterführende Links

- «kes»-/Microsoft-Sicherheitsstudie 2006, <http://www.kes.info/archiv/material/studie2006/>
- BSI-Lagebericht IT-Sicherheit 2007, <http://www.bsi.bund.de/literat/lagebericht/lagebericht2007.pdf>
- MessageLabs Intelligence Special Report; Targeted Attacks April 2007, <http://www.messagelabs.com/mlireport/messagelabs_intelligence_special_report_targeted_attacks_april_2007_5.pdf>
- MessageLabs Intelligence: June 2007 and A2 in Review, <http://www.messagelabs.com/mlireport/MessageLabs%20Intelligence%20-%20Jun%20Q2%20Report%20-%20FINAL.pdf>
- Lageberichte der Melde- und Analysestelle Informationssicherung MELANI, <http://www.melani.admin.ch/dokumentation/00123/00124/index.html?lang=de>
(alle Links letztmals kontrolliert: 29.12.2007).

Zeitschrift für Datenrecht und Informationssicherheit
digma
www.digma.info
erscheint vierteljährlich

Meine Bestellung

❑ 1 Jahresabonnement digma (4 Hefte des laufenden Jahrgangs)
à **CHF 158.00** bzw. bei Zustellung ins Ausland **EUR 123.00** (inkl. Versandkosten)

Name Vorname

Firma

Strasse

PLZ Ort Land

Datum Unterschrift

Bitte senden Sie Ihre Bestellung an:
Schulthess Juristische Medien AG, Zwingliplatz 2, CH-8022 Zürich
Telefon +41 44 200 29 19
Telefax +41 44 200 29 18
E-Mail: zs.verlag@schulthess.com
Homepage: www.schulthess.com

Schulthess §